UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,935	11/23/2005	Carlos Alberto Rega	GJ-263J	2362

7590 10/02/2009

Thomas E Thompkins Jr
Iandiorio & Teska
260 Bear Hill Road
Waltham, MA 02451

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,935	REGA ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,9,15,16,20,23,27-30,33,34,37-40 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,9,15,16,20,23,27-30,33,34,37-40 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 5-8, 10-14, 17-19, 21-22, 24-26, 31-32, 35-36, 41, and 43 have been cancelled.

2. Claims 3-4, 9, 15, 20, 23, 27-30, 33-34, 37-40, and 42 have been amended.

3. Claims 1-4, 9, 15-16, 20, 23, 27-30, 33-34, 37-40, and 42 are pending for consideration.

Priority

4. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Drawings

5. The drawings are objected to because figure 7 is failed to include a system comprising a computer. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the

drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Regarding claim 1, the limitation "the encryption algorithm is selected such that decoding of the encryption algorithm would be ill-conditioned without the constraint" is not clear to the Examiner what the technical meaning of the term "ill-conditioned algorithm" is. Appropriate correction is required.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1-4, 9, 15-16, 20, 23, 27-30, 33-34, and 37-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-4, 9, 15-16, 20, 23, 27-30, 33-34, and 37-40 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process.

11. Claim 1 is directed to a method comprising steps, which is interpreted as software per se, however, the claims fail to assert the program recorded on an appropriate computer-readable medium so as to be structurally and functionally interrelated to the medium and permit the function of the descriptive material to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer without a computer-readable medium needed to realize the computer program's functionality, it is regarded as nonstatutory functional descriptive material. See MPEP 2106.01 for details.

12. The dependent claims are depended on the rejected base claim, and are rejected for the same rationales.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 1-2, 4, 15-16, 20, 23, 27-30 and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by McGough (US 6445797) (hereinafter McGough).

15. Regarding claim 1, McGough discloses a method for encoding and decoding information, the method comprising the steps of: a) using at least one mathematical function (McGough: column 3 lines 45-63); b) producing an encryption algorithm using the mathematical functions such that the algorithm has at least two parameters (McGough: column 8 lines 43-53); c) defining a decode key of a data stream by defining the value of at least one parameter (McGough: column 3 lines 45-63); d) defining information to be carried in a data stream by defining the value of at least one parameters (McGough: column 12 lines 30-50); e) producing a data stream using the encryption algorithm and the defined parameter values (McGough: see figure 1, item 116); and f) decrypting the data stream where the decode key is known and used as a constraint in the

equation such that the information is available, wherein the encryption algorithm is selected such that decoding of the encryption algorithm would be ill-conditioned without the constraint (McGough: column 13 lines 38-61).

16. Regarding claim 2, McGough discloses where at least one of the mathematical functions used in the encryption algorithm is selected to be a non-periodic function (McGough: see figure 2, item 219).

17. Regarding claim 4, McGough discloses where information includes at least one mutation key, and including the step of using the mutation key to effect at least one of the next data stream created or received, the form of ordinate spacing used in the encryption algorithm, the weighting of at least one of the mathematical functions used in the encryption algorithm, the number of mathematical functions used in the encryption algorithm is effected by a mutation key, and at least the type of mathematical functions used in the encryption algorithm (McGough: see figure 2 and column 4 lines 51-58).

18. Regarding claim 15, McGough discloses including the step of the data stream producer decrypting the produced data stream and where decryption fails modifies the value of sat least one parameter used to produce said data stream and produces a second data stream and continues the process until a data stream that correctly decrypts has been produced and discards all data streams that could not be decrypted (McGough: column 26 lines 41-53).

19. Regarding claim 16, McGough discloses where the parameters that are altered to allow a data stream that can be decrypted includes at least one mutation parameters (McGough: column 26 lines 5-13).

20. Regarding claim 20, McGough discloses including the step of allowing a user to select a value and influence the probability that produced data streams cannot be decrypted (McGough: see Abstract section).

21. Regarding claim 23, McGough discloses where at least one of the parameters of the encryption algorithm carries information that may be defined as a password of an external system (McGough: column 22 lines 9-22).

22. Regarding claim 27, McGough discloses where the storage area used to hold at least some of the parameter values that form an authentication key is within the same substrate as the processor which encrypts the messages (McGough: column 22 lines 54-62).

23. Regarding claim 28, McGough discloses which includes the step of including a means to immediately overwrite or flush a temporary data store used in coding or decoding of a data stream (McGough: column 26 lines 41-53).

24. Regarding claim 29, McGough discloses including the step of encrypting the produced data stream using conventional encryption means (McGough: see figure 1).

25. Regarding claim 30, McGough discloses including the step of encrypting at least some of the information prior to it being used to define the values of parameters of the encryption algorithm (McGough: column 21 line 50 through column 22 line 22).

26. Regarding claim 42, McGough discloses apparatus comprising transmitting means receiving means, processing means and operating instructions allowing decryption of a signal according to the method of claim 1 (McGough: see figure 1).

Claim Rejections - 35 USC § 103

27. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. Claims 3 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGough in view of Hur (US 7181620) (hereinafter Hur).

29. Regarding claim 3, McGough does not disclose where the information includes an authentication key, and including the step of validating the authentication key. However, Hur discloses where the information includes an authentication key, and including the step of validating the authentication key (Hur: column 14 lines 34-41). Therefore, it would have been obvious to a person skilled art at the time the invention was made to have included in McGough the feature of Hur as discussed above because there is a need for a way to provide secure key distribution in a manner that offers interoperability among different systems and high performance. There is a need for a system that has greater scalability than a Kerberos system and less administrative costs than a PKI system. There is also a need for a system that is equally useful for inter-network communication and intra-network communication (Hur: column 5 lines 43-53).

30. Regarding claim 40, McGough as modified discloses where the information stored includes that of tokens of value that become the property of the owner of the registration number due to a purchase made by means of the invention where the tokens may be exchanged for further goods or services (Hur: column 14 lines 42-46). The same motivation was utilized in claim 3 applied equally well to claim 40.

31. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over McGough in view of Deering et al. (US 2002/0005854) (hereinafter Deering).

32. Regarding claim 9, McGough does not disclose including the step of limiting the accuracy of the representation of the data stream by using at least truncation of the values of the data stream. However, Deering discloses including the step of limiting the accuracy of the representation of the data stream by using at least truncation of the values of the data stream (Deering: paragraph 0019). Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in McGough the feature of Deering as discussed above because there exists a need for a system and method capable of correcting the problem of false contouring in real-time, and more particularly, in the context of a real-time supersampled graphics system (Deering: paragraph 0018).

33. Claims 33-34 and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGough in view of David (US 2002/0073046) (hereinafter David).

34. Regarding claim 33, McGough does not disclose where authentication between users includes a double handshake protocol. However, David discloses where authentication between users includes a double handshake protocol (David: paragraph 0149). Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in McGough the feature of David as discussed above to provide a system and method that

permits one or more parties to a transaction to have confidence that the other party to the transaction is who he or she purports to be (David: paragraph 0013).

35. Regarding claim 34, McGough as modified discloses that includes the step of issuing a unique registration number to each node (David: paragraph 0030). The same motivation was utilized in claim 33 applied equally well to claim 34.

36. Regarding claim 37, McGough as modified discloses including the step of using a protocol such that a first node who is on contact with both a second and third node may act as a start up host between the second and the third node without a host and so provide a distributed start up means (David: see figure 9). The same motivation was utilized in claim 33 applied equally well to claim 37.

37. Regarding claim 38, McGough as modified discloses including the step of having a plurality of stored starting decode keys between node pairs on each node such that on a communication failure reconnection may occur rapidly (David: paragraph 0115). The same motivation was utilized in claim 33 applied equally well to claim 38.

38. Regarding claim 39, McGough as modified discloses in which the method is used in nested mode such that a first encryption algorithm is used to

authenticate between users and then a second encryption algorithm is used to transfer useful information (David: paragraph 0128: triple-DES).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431